AO 106 (Rev. 01/09) Application for a Search Warrant

United States District Court

for the
Western District of New York

In the Matter of the Search of Information Associated with Snapchat Username:
(Briefly describe the property to be searched or identify the person by name and address.)

that_packersfan

THAT IS STORED AT PREMISES OWNED, MAINTAINED, CONTROLLED, OR OPERATED BY SNAP INC.

Case No. 20-M-134
(Filed Under Seal)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, which is attached hereto and incorporated by reference herein,

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B, which is attached hereto and incorporated by reference herein.

The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of 18 U.S.C. §§ 2251(a), 2252A(a)(2)(A), 2252A(a)(5)(B), and 2261A(2)(B).

The application is based on these facts:

- ☒ continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

JAMES J. DONOGHUE
SPECIAL AGENT
HOMELAND SECURITY INVESTIGATIONS
Printed name and title

Sworn to telephonically.

Date: September 11, 2020

Judge's signature

City and state: Buffalo, New York

HONORABLE H. KENNETH SCHROEDER, JR.
UNITED STATES MAGISTRATE JUDGE
Printed name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, James J. Donoghue, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the Snapchat account identified by Snapchat username "that_packersfan" (the "SUBJECT ACCOUNT") that is stored at premises owned, maintained, controlled, or operated by Snap Inc., a social networking company headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Snap Inc. to disclose to the government records and other information in its possession pertaining to the SUBJECT ACCOUNT.

2. I am a Special Agent (SA) of the United States Immigration and Customs Enforcement (ICE) office of Homeland Security Investigations (HSI) within the Department of Homeland Security (DHS). I have worked for HSI for 12 years. I am currently assigned to Homeland Security Investigations (HSI) in Buffalo, New York. As an HSI Special Agent, I have conducted complex criminal investigations related to immigration violations, human smuggling and human trafficking, money laundering, and child exploitation. My current duties include the enforcement of federal criminal statutes involving child exploitation laws. I also work closely with other law enforcement officers who have engaged in numerous investigations involving child exploitation and child pornography and who have received training in the area of child pornography and child exploitation. I further state that I have training and experience as an HSI

Computer Forensics Agent for 3 years and have knowledge of the computer application Snapchat and how the application processes and saves information.

3. I am familiar with the information contained in this affidavit based upon the investigation I have conducted and based on my conversations with other law enforcement officers involved in this investigation, or who have engaged in numerous investigations involving child exploitation.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, law enforcement officers, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2251(a) [production and attempted production of child pornography], 2252A(a)(2)(A) [distribution and receipt of child pornography], 2252A(a)(5)(B) [possession of child pornography], and 2261A(2)(B) [cyberstalking] have been committed by Dyllan BARBER. There is also probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251(a), 2252A(a)(2)(A), 2252A(a)(5)(B), and 2261A(2)(B) may be located in the SUBJECT ACCOUNT described in Attachment A.

PROBABLE CAUSE

6. On March 11, 2020, Detective Matthew Finnerty of the Cattaraugus County Sheriff's Office conducted an extraction of a minor victim's (V1's) cell phone with the consent of V1 and her father. V1's date of birth is May 6, 2003. V1 lives in Cattaraugus, New York.

7. On April 8, 2020, Detective Heather Price of the Cattaraugus County

Sheriff's Office requested my assistance in reviewing the cell phone extraction data of V1's cell phone. While reviewing the extraction report, I observed several images which appear to be screen captures from a Snapchat text conversation between V1 and Snapchat user "Barber (D)." During this conversation, it appears that "Barber (D)" is threatening V1 to send nude pictures of herself or else "Barber (D)" will publicly post other nude pictures he has of V1. For example, "Barber (D)" informs V1 in the chat "U have till midnight to show me your tits pussy and ass or I'm posting on everything about you too." "Barber (D)" goes on to say, "Better be able to see your face and use 2 fingers to masturbate," and "Where's the titties and ur face I didn't say stop Do u got something other then your fingers to use." It appears from the conversation that V1 complied with "Barber (D)'s" request and sent him nude pictures of herself.

8. On April 16, 2020, Detective Price and I interviewed Dyllan BARBER at his home in Little Valley, New York. BARBER's date of birth is January 27, 2001. BARBER signed a consent form to search his cell phone and allowed me to extract data from his cellphone using forensic software. BARBER waived his Miranda rights and agreed to speak with Detective Price and myself. BARBER stated that the cellphone he is currently using is a new phone. His old phone is broken and "somewhere in his bedroom." BARBER has been using the "new" phone since approximately December 2019.

9. BARBER stated that he knew V1 from school and that she dated his younger brother at one time. BARBER stated that his Snapchat and Instagram usernames are "that_packersfan."

10. Snapchat allows a user to give a nickname to the accounts they receive messages from in order to easily identify who the users of those accounts are. This does not change the

actual account name registered with Snapchat. As a result of my investigation, and as further explained below, I have determined that V1 assigned the name "Barber (D)" to BARBER's "that_packersfan" Snapchat account.

11. During the interview with BARBER, Detective Price and I asked BARBER if he had ever received a nude picture from V1. BARBER stated that he did receive one nude picture from V1 approximately two years earlier (which would have been in approximately April 2018), via Snapchat.

12. I asked BARBER about the text message conversation on V1's phone in which his Snapchat account, "that_packersfan," threatened V1 to send nude pictures of herself. BARBER was aware of the conversation. He stated that his Snapchat account, "that_packersfan," had been "hacked," and that the person who had gained access to his account was responsible for threatening V1. BARBER said that he woke up one morning several months ago and found that his Snapchat account had been logged off on his phone. (Snapchat accounts can only be logged into on one device at a time). He stated that he tried to log into his account, but he could not access it because his password had been changed. BARBER stated that at that time, he sent a request to Snapchat informing it that his account had been hacked. BARBER stated that he thinks the "hacker" was able to access his account because his account password was easy to guess. He also stated that based on the time shown in the screen captures of the threatening conversation, he could not have been a party to the conversation because he would have been in bed already.

13. On May 20, 2020, HSI conducted a forensic interview of V1. The interviewer showed V1 printed copies of the screen captures that were found on her phone depicting the

threatening Snapchat conversation. V1 stated that the screen captures depict a Snapchat conversation she had with BARBER's Snapchat account. V1 stated, "I think that Dyllan was pretending to be someone he was not. He said he would post a nude picture of me on his Snapchat if I didn't send him another picture of me. I was scared. I told dad. He said if it ever happens again, come to me."

14. On July 1, 2020, Detective Price and I interviewed V1 and asked her if she knows someone named Dyllan BARBER. V1 stated that BARBER is her ex-boyfriend's brother. V1 stated that BARBER's Snapchat username is "that_packersfan." V1 stated that she sent nude pictures of herself to BARBER during a Snapchat conversation in which she was threatened to send nude pictures. When asked how many pictures she sent, she stated, "a lot." When asked why she believed the user of the account that threatened her was in possession of other nude pictures of her, V1 said that she did not know how the user could have received other nude pictures of her, she just believed him when he told her that he had them and would share them with the public.

15. V1 further stated that she was on a phone call with BARBER during the threatening Snapchat conversation. During the call, BARBER told V1 to "just take them," meaning take and send nude pictures of herself. BARBER further told V1 that he was concerned that the hacker would also post nude pictures of BARBER. According to V1, BARBER did not want V1 to talk to V1's father about what had happened because he did not want to get into trouble. V1's father works in law enforcement.

16. Based on my review of the file creation dates of the screen capture images located on V1's cell phone and the phone call records between V1 and BARBER located on V1's cell

phone, the threatening Snapchat conversation appears to have taken place sometime in November 2019. Specifically, the screen captures appear to have been taken between November 30, 2019 at 8:29:50 PM and December 1, 2019 at 10:02:08 AM. A total of nineteen screen captures depict the conversation. The time on the phone can be seen within the screen captures, giving a possible time that the screen captures were taken. The time frame for the screen captures is between 8:20 and 11:01. It is not known if this is AM or PM, and a date is not visible in the screen captures.

17. Phone records obtained from V1's cell phone indicate that there are several incoming and outgoing phone calls from November 27 through November 30, 2019 between V1 and a contact in her phone designated "Dyllan Barber" with phone number 716-801-3290.

BACKGROUND ON SNAPCHAT

18. Snapchat is a free-access social-networking application that can be accessed as a mobile application on a cell phone or other electronic device capable of downloading the social media application. Snapchat allows its users to create their own profile with a photo of themselves, and other information. Snapchat is owned and maintained by Snap Inc., a company headquartered in Santa Monica, California.

19. The users of Snapchat communicate with other Snapchat users by sending photos or videos to one another. When an image or video ("snap") is sent to another Snapchat user, the person sending the image can set a timer on the image to determine when the image will automatically delete after the receiving Snapchat user receives the image. In many cases, the images will automatically delete in 10 seconds. The user sending an image can set the automatic delete setting on the image from 1 second to 10 seconds, or the option to never

delete once sent to the other Snapchat user. Once an image automatically deletes, the receiving user of the image will no longer be able to see or watch the sent image.

20. If a Snapchat user receiving an image wants to save the image sent to them, the receiving user can quickly capture the image by saving the image once it is opened by the receiving user on Snapchat. If a receiving user on Snapchat saves the image sent to them, the sending user on Snapchat will receive a notification that the Snapchat user who received their image took a screen capture or saved the image that was sent to them. However, this screen capture auto notification can be bypassed if the receiving user takes a photo of their screen by using a separate camera or other electronic device to capture the sent image.

21. Snapchat also allows users to add "filters" to photos taken within the Snapchat application. This filter can add animal characteristics to the user who is taking a photo of themselves or other people in the photo. The filters can also allow the user to take a video of themselves with a voice changer. Other filters within Snapchat can add locations where the images were taken based on the user's physical location if GPS (Global Positioning System) is activated on the Snapchat user's device. This type of information is referred to by Snapchat as Location Data and further described below.

22. Snapchat users can also post daily images taken within the Snapchat application allowing the user to document their daily activity. These daily images are documented in the Snapchat "Story." Many users of Snapchat post daily consecutive images in an attempt to show their daily usage of the Snapchat mobile application. These daily postings of images are often referred to as "Streaks."

23. Snaps are photos or videos taken using the Snapchat app's camera on an individual's mobile device, and may be shared directly with the user's friends, or in a Story

(explained below) or Chat. Snapchat's servers are designed to automatically delete a Snap after it has been viewed by all intended recipients. Snapchat's servers are designed to automatically delete an unopened Snap sent directly to a recipient after 30 days and an unopened Snap in Group Chat after 24 hours.

24. A user can add Snaps to their "Story." A Story is a collection of Snaps displayed in chronological order. Users can manage their privacy settings so that their Story can be viewed by all Snapchatters, their friends, or a custom audience. A user can also submit their Snaps to a crowd-sourced service, "Our Story," which enables their Snaps to be viewed by all Snapchatters in Search and Snap Map.

25. Snapchat's servers are designed to automatically delete a Snap in a user's Story 24 hours after the user posts the Snap, but the user may delete part or all of the Story earlier. Submissions to "Our Story" may be saved for longer periods of time.

26. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone's photo gallery in "Memories." Content saved in Memories is backed up by Snapchat and may remain in Memories until deleted by the user. Users may encrypt their content in Memories (called "My Eyes Only"), in which case the content is not accessible to Snapchat and cannot be decrypted by Snapchat.

27. A user can type messages, send Snaps, audio notes, and video notes to friends within the Snapchat app using the Chat feature. Snapchat's servers are designed to automatically delete one-to-one chats once the recipient has opened the message and both the sender and recipient have left the chat screen, depending on the user's chat settings.

28. Snapchat's servers are designed to automatically delete unopened one-to-one chats in 30 days. Users can also chat in groups. Chats sent in groups are deleted after 24 hours

whether they are opened or not. A user can save a message in Chat by pressing and holding the message. The user can unsave the message by pressing and holding it again. This will delete it from Snapchat's servers. Users can also delete chats that they have sent to a recipient before the recipient has opened the chat or after the recipient has saved the chat.

29. If a user has device-level location services turned on and has opted into location services on Snapchat, Snapchat will collect location data at various points during the user's use of Snapchat, and retention periods for location data vary depending on the purpose of the collection. Users have some control over the deletion of their location data in the app settings.

30. Snapchat asks users to provide basic identity and contact information upon registration and also allows users to provide additional identity information for their user profile. This information may include the user's full name, e-mail addresses, and phone numbers, as well as potentially other personal information provided directly by the user to Snapchat. Once an account is created, users may also adjust various privacy and account settings for the account on Snapchat. These account settings can include limiting the Snapchat application to access the cell phone's camera, microphone, and/or lists of names and phone numbers listed in the Contact List of the cell phone. This information regarding other Snapchat users is collected and maintained by Snapchat.

31. Snapchat allows users to have "friends," which are other individuals with whom the user can share information without making the information public. Friends on Snapchat may come from either contact lists maintained by the user, users inputted by the account owner, other third-party social media websites and information, or searches conducted by the user on Snapchat profiles. This information is collected and maintained by Snapchat.

32. Snapchat allows users to post and share various types of user content, including

photos, videos, comments, and other information. User content that is posted within Snapchat or shared through Snapchat is collected and maintained by Snapchat.

33. Users on Snapchat may also search Snapchat for other users by searching for a specific user's name known to the user or by scanning the other Snapchat users "Snapcode" code. A Snapcode is similar to a QR Code, which is a type of unique image which identifies a Snapchat user's profile on Snapchat to one user. This allows users to share their identity with other Snapchat users with a simple image, without sharing a username or any other personally identifying information such as a phone number or an email address.

34. For each user, Snapchat also collects and retains information, called "log file" information, every time a user requests access to Snapchat, whether to login to the application or to logout of the application. Among the log file information that Snapchat's servers automatically record is the particular Internet Protocol ("IP") address associated with the request. If the IP access is made with a cellular telephone, some information obtained by Snapchat will capture the actual "IP6" (IP version6) data, which is capable of capturing the information related to a specific mobile or electronic device, including dates and times of access to the Snapchat account, and other information.

35. Snapchat users can also communicate privately with other Snapchat users, or they can communicate within "groups" of other Snapchat users who all have the Snapchat application on their electronic devices. Users can share photos, videos, and personal messages to one another within the application which cannot be viewed by other users within the same application.

36. Snapchat also may communicate with the user. Snapchat collects and maintains copies of communications between Snapchat and the user.

37. Based on the information above, the computers of Snap Inc. are likely to contain all the material described above with respect to the SUBJECT ACCOUNT, including stored electronic communications and information concerning the subscriber and their use of Snapchat, such as account access information, which would include information such as the IP addresses and devices used to access the SUBJECT ACCOUNT, as well as other account information that might be used to identify the actual user or users of the SUBJECT ACCOUNT at particular times.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

38. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Snap Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

39. Based upon the foregoing information, the undersigned respectfully submits that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251(a), 2252A(a)(2)(A), 2252A(a)(5)(B), and 2261A(2)(B) may be located in the SUBJECT ACCOUNT described in Attachment A.

40. Based upon the foregoing, I respectfully request that the Court issue the proposed search warrant.

41. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant

by serving the warrant on Snap Inc. Because the warrant will be served on Snap Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

42. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation the scope of which is neither public nor known to the target of the investigation. Additionally, these documents contain information relating to the identity of a minor victim. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize the investigation and reveal information concerning a minor victim.

James J. Donoghue
Special Agent
Homeland Security Investigations

Sworn to telephonically
this 11th day of September, 2020

HON. H. KENNETH SCHROEDER, JR.
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Snapchat account identified by Snapchat username "that_packersfan" (the "SUBJECT ACCOUNT") that is stored at premises owned, maintained, controlled, or operated by Snap Inc., a company located at 2772 Donald Douglas Loop North, Santa Monica, CA 90405.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Snap Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Snap Inc., including any messages, records, files, logs, or information that have been deleted but are still available to Snap Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Snap Inc. is required to disclose the following information to the government for the SUBJECT ACCOUNT listed in Attachment A, regardless of whether such information is located within or outside the United States, within 14 days of service of this warrant:

a. All identity and contact information for the SUBJECT ACCOUNT, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;

b. All past and current usernames, account passwords, and names associated with the SUBJECT ACCOUNT, including the dates on which such usernames, account passwords, and names were in usage;

c. All photographs and images in the user gallery for the SUBJECT ACCOUNT;

d. The dates and times at which the SUBJECT ACCOUNT and profile were created, and the Internet Protocol ("IP") address at the time of sign-up, and any IP addresses associated with attempted logins;

e. For the time period April 1, 2018 through December 31, 2019, all IP logs and other documents showing the IP address, date, and time of each login to the SUBJECT ACCOUNT, as well as any other log file information;

f. For the time period April 1, 2018 through December 31, 2019, all information regarding the particular device or devices used to login to or access the SUBJECT ACCOUNT, including all device identifier information or cookie information, including all information about the particular device or devices used to access the SUBJECT ACCOUNT and the date and time of those accesses;

g. All data and information associated with the profile page for the SUBJECT ACCOUNT, including photographs, "bios," and profile background and themes;

h. For the time period April 1, 2018 through December 31, 2019, all communications or other messages sent or received by the SUBJECT ACCOUNT;

i. For the time period April 1, 2018 through December 31, 2019, all user content created, uploaded, or shared by the SUBJECT ACCOUNT, including any comments made by the SUBJECT ACCOUNT on photographs or other content;

j. For the time period April 1, 2018 through December 31, 2019, all photographs and videos that have been sent and/or received by the SUBJECT ACCOUNT;

k. For the time period April 1, 2018 through December 31, 2019, all location data associated with the SUBJECT ACCOUNT, including geotags and/or metadata associated with the photos and/or videos that were sent/received, even if the metadata was removed by Snap Inc. upon receipt of either the photos or videos;

l. For the time period April 1, 2018 through December 31, 2019, all data and information that has been deleted by the user(s) of the SUBJECT ACCOUNT;

m. A list of all of the people that the SUBJECT ACCOUNT follows on Snapchat and all people who are following the SUBJECT ACCOUNT *(i.e.,* "friends" list and "followers" list), as well as any friends of the SUBJECT ACCOUNT;

n. A list of all users that the SUBJECT ACCOUNT has "unfollowed" or blocked;

o. All privacy and account settings;

p. For the time period April 1, 2018 through December 31, 2019, all records of Snapchat searches performed by the SUBJECT ACCOUNT, including all past searches saved by the SUBJECT ACCOUNT;

q. For the time period April 1, 2018 through December 31, 2019, all information about connections between the SUBJECT ACCOUNT and third-party websites and applications; and

r . For the time period April 1, 2018 through December 31, 2019, all records pertaining to communications between Snapchat and any person regarding the user or the user of the SUBJECT ACCOUNT, including contacts with support services, and all records of actions taken, including suspensions of the account.

II. Information to be searched for and seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2251(a), 2252A(a)(2)(A), 2252A(a)(5)(B), and 2261A(2)(B), including, for the SUBJECT ACCOUNT identified in Attachment A, information pertaining to the following matters:

a. All communications or other messages sent from or received by the SUBJECT ACCOUNT, including comments and direct messages, and all associated multimedia;

b. All content created, uploaded, received, or shared by the SUBJECT ACCOUNT, including all videos, images, and all associated metadata;

c. All photographs and images;

d. Evidence indicating how and when the SUBJECT ACCOUNT was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crimes under investigation and to the account user;

e. Evidence indicating the SUBJECT ACCOUNT user's state of mind as it relates to the crimes under investigation; and

f. The identity of the person(s) who created or used the SUBJECT ACCOUNT.